

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	DATE FILED:
v.	:	CRIMINAL NUMBER:
ALLAN ERIC CARLSON	:	CHARGES: 18 U.S.C.
	:	§ 1030(a)(5)(A)(i) (Computer
	:	fraud) - 26 counts
	:	18 U.S.C.
	:	§ 1030(a)(5)(A)(ii) (Computer
	:	fraud) - 26 counts
	:	18 U.S.C.
	:	§ 1028(a)(7) (Identification
	:	information fraud) - 27 Counts
	:	Notice of forfeiture
	:	

INDICTMENT

COUNTS ONE THROUGH ELEVEN

THE GRAND JURY CHARGES:

Introduction

1. At all times material to this indictment, the defendant ALLAN ERIC CARLSON was an individual who resided at 1232 East Lexington Drive, Glendale, CA 91206.

2. At all times material to this indictment, the defendant ALLAN ERIC CARLSON possessed a computer and had access to the Internet through MindSpring, an Internet Service Provider (ISP). MindSpring was owned by EarthLink, another ISP.

3. As is further described in this indictment, the defendant ALLAN ERIC CARLSON violated various federal criminal statutes by “hacking,” that is, gaining unauthorized access to the computers of other persons on the Internet; sending thousands of e-mail messages from the

victim's computers; and "spoofing," that is, falsifying the return addresses of these e-mails, which caused a "distributed denial of service" (DDoS) attack upon the computer systems of the persons whose e-mail addresses he had spoofed.

Definitions of Terms Used in this Indictment

4. When the following terms are used in this indictment, they are defined as follows:

a. Addresses

Every device on the Internet has an address that allows other devices to locate and communicate with it. An Internet Protocol (IP) address is a unique number that identifies a device on the Internet. (See Paragraph 4.i, below.) Other addresses include Uniform Resource Locator (URL) addresses, such as "http://www.usdoj.gov," which are typically used to access web sites or other services on remote devices. Domain names, host names, and machine addresses are other types of addresses associated with Internet use.

b. Denial of Service Attack (DoS Attack)

A person attempting a DoS Attack will send a particular computer on the Internet hundreds or thousands of messages in a short period of time. The attacked computer will devote system resources to each transmission. Due to the limited resources of computers, this bombardment will eventually slow the victim computer down and may eventually cause it to fail ("crash") altogether.

c. Distributed Denial of Service Attack (DDOS)

A person attempting a DoS attack may enlist other computers, without the knowledge of the owners, to assist in the attack by causing other computers to bombard the target

computer at the same time. This increases the number of messages that can be directed to the victim computer and increases the chances of slowing the victim computer and crashing it.

d. Domain

A domain is a group of Internet devices that are owned or operated by a specific individual, group, or organization. Devices within a domain have IP addresses within a certain range of numbers, and are usually administered according to the same set of rules and procedures.

e. Domain Name

A domain name identifies a computer or group of computers on the Internet, and corresponds to one or more IP addresses within a particular range. Domain names are typically strings of alphanumeric characters, with each “level” of the domain delimited by a period (e.g., Computer.networklevel1.networklevel2.com). A domain name can provide information about the organization, ISP, and physical location of a particular network user. Two domain names relevant to this indictment are phillynews.com, the domain name of Philadelphia Newspapers, Inc. and phillies.com, the domain name of the Philadelphia Phillies baseball team.

f. Header Information

When information is sent over the Internet, the computer transmits the information and places a “header” on each packet of information. The header contains information identifying the sending computer and the receiving computer and also contains

information that tells the receiving computer what kind of information the packet contains (e.g., e-mail, request for a web page, etc.)

g. Internet

The Internet is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions.

h. Internet Service Providers (“ISPs”)

Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers (“ISPs”). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

i. IP Address

The Internet Protocol address (or “IP address”) is a unique numeric address used by computers on the Internet. It is the computer equivalent of a telephone number. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned a unique IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

- (1) Dynamic IP address. When an ISP or other provider uses dynamic IP addresses, the ISP randomly assigns one of the available IP addresses in the range of IP addresses controlled by the ISP each time a connects with the ISP to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who connect at a later time. Thus, an individual customer's IP address normally differs each time he uses the ISP service.
- (2) Static IP address. A static IP address is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will always have the same IP address.

j. Log File

Log files are computer files that contain records about system events and status, the activities of users, and anomalous or unauthorized computer usage.

k. Ports

A port is a process that permits the operating system of a computer to know what to do with incoming traffic. A computer does not have physical ports. Rather, a port is a process that permits the computer to process information as it arrives at the computer. All incoming traffic has a “header” as well as its content. Part of the header information identifies the port to which the incoming information is addressed. For example, Port 80 is, by convention, website traffic. As a packet of information is received, the computer operating system notes that it is addressed to Port 80 and sends the packet to the web operating software. Similarly, Port 25 is for incoming e-mail. When the operating system sees a packet of information addressed to Port 25, it directs the packet to the e-mail software.

l. Router

A router is a device on the Internet that facilitates communication. Each Internet router maintains a table that states the next step a communication must take on its path to its proper destination. When a router receives a transmission, it checks the transmission's destination IP address with addresses in its table, and directs the communication to another router or the destination computer.

m. Server

A server is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called “clients.” In a large company, it is common for individual employees to have client

computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a “web server.” Similarly, a server that only stores and processes e-mail is known as a “mail server.”

n. Tracing

Trace programs are used to determine the path that a communication takes to arrive at its destination. A trace program requires the user to specify a source and destination IP address. The program then launches a message from the source address, and at each “hop” on the network (signifying a device such as a router), the IP address of that device is displayed on the source user's screen or copied to a log file.

o. User Name or User ID

Most services offered on the Internet assign users a name or ID, which is a pseudonym that computer systems use to keep track of users.

THE DEFENDANT’S E-MAIL ATTACK SCHEME

5. From in or about November 2001 to in or about December 2002, the defendant ALLAN ERIC CARLSON collected e-mail addresses of computer users on the Internet. The defendant then sought out computers that were connected to the Internet and looked for those with open ports that would allow him access to the computer. After the defendant gained access

to these computers, without the knowledge of the owners, and he composed e-mails, mostly regarding the Philadelphia Phillies baseball team. When he composed these e-mails, the defendant frequently created a return address that belonged to yet another computer user, without that user's knowledge or consent. (This is known as "spoofing" an e-mail address.) Most often the defendant spoofed the e-mail addresses of sports writers at the Philadelphia Daily News and the Philadelphia Inquirer, two newspapers owned by Philadelphia Newspapers, Inc. (PNI), which is, in turn, owned by Knight-Ridder, Inc. The defendant then sent these e-mails to thousands of e-mail addresses that he had collected.

6. Many of the e-mail addresses to which the defendant ALLAN ERIC CARLSON sent his e-mails were not valid addresses. When a server receives an e-mail addressed to an invalid address, it sends the e-mail to the return address. Thus, when the defendant spoofed return addresses, the persons whose address were spoofed received all of the messages that were addressed to invalid addresses. This resulted in a Distributed Denial of Service (DDOS) attack on the servers on which the spoofed e-mail address holders had their accounts, by sending thousands of messages to individual computer mailboxes in a short period of time.

THE SPECIFIC ATTACKS

Attack of November 7, 2001

7. On or about November 7, 2001, the defendant ALLAN ERIC CARLSON gained access to a computer in Canada over the Internet without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Canada was assigned an IP address that was assigned to Shaw Communications, a

Canadian ISP, for reassignment to its customers. The subject of the e-mail was “The Mariner’s Didn’t Trade A-Rod.” The defendant gave the e-mail a false and non-existent return address of SpecialProsecutor@fbi.gov and sent it to PNI writers B.B., S.D., P.H., R.H., D.B. and J.H. Each of them received this e-mail approximately 1168 times. The text of the e-mail message was:

The Mariners didn’t trade A-Rod.
The Phillies payroll should be over \$100mil and you know it.
You belong in prison with the Phillies owners.

Attack of November 11, 2001

8. On or about November 11, 2001, the defendant ALLAN ERIC CARLSON gained access to a computer in Canada over the Internet without the knowledge of the owner and launched an e-mail attack on by sending thousands of e-mails. At the time of the attack, the computer in Canada was assigned an IP address that was assigned to Shaw Communications for reassignment to its customers. The subject of the e-mail was “Sign JASON GIAMBI.” As a result of this attack, the Phillies server received numerous copies of this e-mail.

Attack of November 13, 2001

9. On or about November 13, 2001, the defendant ALLAN ERIC CARLSON gained access to a computer in Canada over the Internet without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Canada was assigned an IP address that was assigned to Shaw Communications for reassignment to its customers. The subject of the e-mail was “Your Offense Blows Goats.” As a result of this attack, the Phillies server received numerous copies of this e-mail.

Attack of November 16, 2001

10. On or about November 16, 2001, the defendant ALLAN ERIC CARLSON gained access to a computer in Canada over the Internet without the knowledge of the owner and launched an e-mail attack on PNI and the Phillies by sending thousands of e-mails. At the time of the attack, the computer in Canada was assigned an IP address that was assigned to Shaw Communications for reassignment to its customers. The subject of the e-mail was "Rolen Speaks." CARLSON used an e-mail address of an account at the University of Pennsylvania to spoof the return address of the e-mail. The e-mail was sent to PNI writers B.B., S.D., P.H., R.H., D.B., J.H. and B.L. Each of them received approximately 402 copies of this e-mail. In addition, approximately 800 copies of this e-mail were sent to an e-mail address at the Phillies. The person at the University of Pennsylvania whose return address was spoofed also received numerous copies of this e-mail as they were "bounced" from "bad addresses."

Attack of November 18, 2001

11. On or about November 18, 2001, the defendant ALLAN ERIC CARLSON gained access to a computer in Canada over the Internet without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Canada was assigned an IP address that was assigned to Shaw Communications for reassignment to its customers. The subject of the e-mail was "EAT SHIT AND DIE." The e-mail spoofed the return address of an e-mail account at Denison University, in Ohio. The e-mail was sent to PNI writers B.B., S.D., P.H., R.H., D.B., J.H. and B.L. Each of them received approximately 894 copies of this e-mail.

12. On or about November 18, 2001, the defendant ALLAN ERIC CARLSON gained access to a computer in Canada over the Internet without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Canada was assigned an IP address that was assigned to Shaw Communications for reassignment to its customers. The subject of the e-mail was “It’s The Payroll Stupid.” The e-mail spoofed the return address of an e-mail account at webtv.net. The e-mail was sent to PNI writers B.B., S.D., P.H., R.H., D.B., J.H. and B.L. Each of them received approximately 1304 copies of this e-mail.

Attack of November 19, 2001

13. On or about November 19, 2001, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Canada without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Canada was assigned an IP address that was assigned to Shaw Communications, for reassignment to its customers. The subject of the e-mail was “Rolen is the Franchise.” The e-mail was sent from the computer in Canada, but the defendant spoofed the return address of P.H., a sports writer at PNI. As a result, approximately 6,638 copies of this e-mail were “bounced” to the e-mail box of P.H. The Phillies e-mail server also received numerous copies of this e-mail message.

Attack of November 20, 2001

14. On or about November 20, 2001, the defendant ALLAN ERIC CARLSON gained access to a computer in Long Island, NY, without the knowledge of the owner and launched an

e-mail attack. At the time of the attack, the computer in Long Island was assigned an IP address that was assigned to an ISP named Cablevision for reassignment to its customers. The subject of the e-mail was “No Giambi=No Rolen.” The defendant spoofed the return address of an e-mail account at sportstease.com. The e-mail was sent to PNI writers B.B., S.D., P.H., R.H., D.B., J.H. and B.L. Each of them received approximately 905 copies of this e-mail.

Attack of December 3, 2001

15. On or about December 3, 2001, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Long Island, NY, without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Long Island was assigned an IP address that was assigned to an ISP named Cablevision for reassignment to its customers. The subject of the e-mail was “Pat Burrell Hates Philadelphia.” The e-mail was sent from the computer in Long Island, but the defendant spoofed the return address of P.H. As a result, approximately 6,638 copies of this e-mail were “bounced” from “bad addresses” to the e-mail box of P.H.

Attack of December 9, 2001

16. On or about December 9, 2001, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Long Island, NY, without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Long Island was assigned an IP address that was assigned to Cablevision for reassignment to its customers. The e-mail did not have a subject. The e-mail was sent from the computer in Long Island, but the defendant again spoofed the return address of B.B., a sports

writer with PNI. As a result, approximately 2,217 copies of this e-mail were “bounced” to B.B.’s e-mail box.

Attack of December 10, 2001

17. On or about December 10, 2001, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Long Island, New York without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in Long Island was assigned an IP address that was assigned to Cablevision for reassignment to its cable modem customers. The defendant sent thousands of copies of an e-mail with the subject “Phillies Terrified of Rolen.” The message criticized the Philadelphia Phillies baseball team's handling of certain player personnel. The defendant again spoofed the return address of P.H. As a result, approximately 5,560 e-mail messages were “bounced” from “bad addresses” to the e-mail box of P.H.

Attack of December 11, 2001

18. On or about December 11, 2001, the defendant ALLAN ERIC CARLSON sent thousands of copies of an e-mail criticizing the Philadelphia Phillies baseball team's handling of certain player personnel. The subject was “The Scam Continues To Expand.” These e-mails were sent from the same IP address, used in the attack of December 10, 2001. The defendant spoofed return e-mail address of B.L., a sports writer with PNI. As a result approximately 6,865 e-mail were “bounced” from “bad addresses” to B.L.’s e-mail box.

Attack of January 20, 2002

19. On or about January 20, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. The computer had an IP address that is assigned to a Brazilian ISP for reassignment to its customers. The defendant spoofed the return e-mail address of B.B. and the e-mail was on the subject, "The Rotation." On or about January 20, 2002 B.B. received approximately 2,716 "bounced" copies of this e-mail in his e-mail box.

Attack of January 24, 2002

20. On or about January 24, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer over the Internet without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. The computer had the same IP address as the one involved in the attack of January 20, 2002. The e-mails had the spoofed return address of B.B. and contained more complaints about the Phillies. On or about January 24, 2002, B.B. received approximately 3,388 "bounced" copies of this e-mail in his e-mail box.

Attack of February 19-20, 2002

21. Between on or about February 19, 2002 and on or about February 20, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. This computer was connected to the ISP Speakeasy Network for reassignment to its customers. The e-mails had the spoofed return addresses of the PNI staff members listed below

in Paragraph 22. As a result of this attack, each of the staff members received numerous “bounced” copies of the e-mail message.

22. On or about February 20, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. This computer was connected to the ISP Comcast Cablevision for reassignment to its customers. The e-mails had the return addresses of the PNI staff members listed below and was on the subject, “Why the Phillies Suck.” As a result of this attack, each of the staff members received numerous “bounced” copies of the e-mail message.

<u>Name</u>	<u>Approximate Number. of messages</u>	<u>Approximate Time</u>	<u>ISP</u>
T.D.	593	2:00 AM	Speakeasy Network
B.M.	1,149	2:52 AM	Speakeasy Network
P.M.	1,083	1:15 AM	Speakeasy Network
J.M.	2,136	5:20 AM	Speakeasy Network
A.M.	2,065	11:29 AM	Speakeasy Network
L.S.	2,794	12:13 AM	Speakeasy Network
A.R.	380	1:31 PM	Comcast
C.S.	1,894	2:39 PM	Comcast
G.S.	1,427	4:07 PM	Comcast
T.S.	1,575	5:48 PM	Comcast
J.T.	1,327	6:44 PM	Comcast
R.T.	1,149	7:59 PM	Comcast
F.V.	1,358	8:44 PM	Comcast
R.W.	2,606	10:10 PM	Comcast
TOTAL	21,536		

Attack of February 26-28, 2002

23. Between or about February 26, 2002 and on or about February 28, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to the computer of a customer of Comcast Cable. Without the knowledge of the owner, he launched an e-mail attack by sending thousands of e-mail messages on the subject "Tired of the Bullshit." CARLSON spoofed the return addresses of two e-mail boxes at the Philadelphia Phillies. As a result, the Phillies e-mail server received approximately 14,000 copies of this e-mail.

Attack of March 12, 2002

24. On or about March 12, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Canada without the knowledge of the owner. The computer was assigned an IP address that was assigned to Cogeco Cable for reassignment to its customers. The message was on the subject, "Where's Brian Giles." CARLSON spoofed the return address of an e-mail account at phillies.com. This e-mail was sent only to two other e-mail boxes at phillies.com and each of those e-mail boxes received approximately 1,800 "bounced" copies of the message.

25. On or about the same date and from the same computer, the defendant ALLAN ERIC CARLSON launched an e-mail attack on the subject "Why Burrell is Crap." This e-mail was sent to thousands of people. CARLSON spoofed a return address of an e-mail account at the Phillies. As a result that e-mail box received approximately 13,000 "bounced" copies of this e-mail.

Attack of March 13-14, 2002

26. Between or about March 13, 2002, and on or about March 14, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Canada without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. The computer in Canada had an IP address that is assigned to Le Groupe Vidéotron, Ltée, a Canadian ISP for reassignment to its customers. The e-mail had the spoofed return address of L.S., an editor at PNI, and was on the subject, "The Color of Crime." On or about March 14, 2002, approximately 5,514 "bounced" copies of this e-mail were sent to the e-mail box of L.S.

Attack of April 9, 2002

27. On or about April 9, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Canada without the knowledge of the owner and launched an e-mail attack on J.L. of Hazleton, PA, by sending thousands of e-mails. The computer belonged to the same customer of Cogeco Cable that had been involved in the attack of March 12, 2002. The defendant sent thousands of copies of an e-mail, which copied an Internet bulletin board posting that J.L. had made a few days earlier. However, at the end of the message, Carlson added the words, "If you would like to be removed from this mailing, please click reply and include your name, address, Social Security # and date of birth so we can verify your identity." These e-mails had a spoofed return address of J.L., who hosted an Internet website devoted to discussion of the Philadelphia Phillies. As a result, more than 7,000 "bounced" e-mail messages were sent to the e-mail box of L.L.

Attack of June 17, 2002

28. On or about June 17, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Long Island, New York without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. At the time of the attack, the computer in New York was assigned an IP address belonging to Cablevision and was reassigned to one of its customers. The e-mails had the spoofed return address of the account of sports writer P.H. at PNI and the subject was "Corrupt Philly Media Keeps Phils in Cellar." On or about June 17, 2002, P.H. received approximately 10,750 "bounced" copies of this e-mail in his e-mail box at phillynews.com.

Attempted Attack of June 19, 2002

29. On or about June 19, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to the same computer as he did on June 17, 2002, without the knowledge of the owner, and launched another e-mail attack. The e-mail was sent from the computer in Long Island, New York, but the defendant gave it a spoofed return address at PNI that did not exist. The subject line of the e-mail was "Giles Time in Pittsburgh Almost Up" and concerned Brian Giles, a player on the Pittsburgh Pirates baseball team. Many people received this e-mail. However, because the return e-mail address did not exist, there was no flood of e-mails in any box at the PNI server.

Attacks of the week of July 1, 2002

30. On or about July 1, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Canada without the knowledge of the

owner and launched an e-mail attack by sending thousands of e-mails. The computer in Canada was assigned an IP address belonging to Vidéotron Canada, a Canadian ISP. The subject of the e-mail was “Dave Montgomery Must Go.” The e-mail was sent from the computer in Canada, but the defendant gave it a spoofed return address of C. S., an editor at PNI.

31. On or about July 2 and July 3, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer in Canada without the knowledge of the owner and launched another e-mail attack on PNI by sending thousands of e-mails. The computer in Canada was assigned an IP address belonging to Cogeco Cable. The subject of the e-mail was again, “Dave Montgomery Must Go,” and the text of the e-mail was the same as the one sent on or about July 1, 2002. The e-mail was sent from the computer in Canada, but the defendant gave it a spoofed return address of C.S. As a result, of these two attacks, approximately 41,870 copies of this e-mail were “bounced” to the e-mail box of C.S.

Attack of July 14-15, 2002

32. On or about July 14 and 15, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Comcast without the knowledge of the owner and launched another e-mail attack by sending thousands of e-mails. The subject of the e-mail was “Trade Pat Burrell Now.” CARLSON spoofed the return address of P.M., a sportswriter for PNI.

Attack of July 17, 2002

33. On or about July 17, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Cogeco Cable in

Canada without the knowledge of the owner and launched another e-mail attack by sending thousands of e-mails. The e-mail message was the same as the one sent on or about July 14 and 15, 2002, and had the same spoofed return address. As a result of these two attacks, approximately 12,611 copies of this e-mail were “bounced” in the e-mail box of P.M.

Attack of July 20, 2002, and July 23, 2002

34. On or about July 20, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Charter Communications, Inc. in St. Louis, MO, without the knowledge of the owner and launched an e-mail attack by sending thousands of e-mails. The subject of the e-mail was “No Buyers for Phillies Stadium Naming Rights.” It discussed the defendant’s theory why no company would purchase the naming rights to the Philadelphia Phillies' new baseball stadium. The e-mail was sent from the computer of a Charter Communications subscriber, but the defendant gave it a return address of R.W., a sports writer with PNI.

35. On or about July 23, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Cogeco Cable and, without the knowledge of the owner, sent the same e-mail that he had sent on or about July 20, 2002. As a result of these two attacks, more than 57,000 copies of this e-mail were “bounced” to the e-mail account of R.W.

Attack of August 1, 2002

36. On or about August 1, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer and launched another e-mail attack by

sending thousands of e-mails. The subject line was, “The Next GM.” The spoofed return address was an account at the Phillies server. As a result of this attack, the Phillies server received approximately 25,000 copies of this e-mail that were “bounced” to it.

Attack of August 4, 2002

37. On or about August 4, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Charter Communications, Inc., without the permission of the owner, and launched another e-mail attack. This one was captioned “The Smoking Gun” and continued to discuss the Phillies and the coverage by the Philadelphia newspapers. The attack spoofed the return e-mail address of P.L., an officer of Knight-Ridder (the parent company of PNI). As a result, approximately 12,000 copies of this e-mail were “bounced” to the e-mail account of P.L.

Attack of August 14 and 15, 2002

38. On or about August 14, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Cogeco Cable, without the permission of the owner, and launched another e-mail attack. The defendant spoofed the e-mail address of H.S., an officer of Knight-Ridder Digital. The subject of this e-mail was “Time to Clean House” and was another e-mail about the Philadelphia Phillies.

39. On or about August 15, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to the same computer and launched another e-mail attack using the same message and the same spoofed return address as he had on or about August 14,

2002. As a result, approximately 12,000 copies of this e-mail were “bounced” to the e-mail account of H.S.

Attack of August 27-28, 2002

40. On or about August 27, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Cablevision, without the permission of the owner, and launched another e-mail attack. CARLSON spoofed the return e-mail address of K.R., a reporter at The Sporting News. This e-mail was captioned “Bill Conlin's work” and contained complaints about the sports writing of Bill Conlin and his failure to criticize the Philadelphia Phillies baseball team for the way that they handle their payroll.

41. On or about August 28, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Cable One, without the permission of the owner, and launched another e-mail attack. He again spoofed the return e-mail address of K.R. This e-mail was captioned “Bill Conlin's work” and contained complaints about the sports writing of Bill Conlin and his failure to criticize the Philadelphia Phillies baseball team for the way that they handle their payroll.

42. On or about August 28, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of AT&T Broadband, without the permission of the owner, and launched another e-mail attack. He again spoofed the return e-mail address of K.R. This e-mail was captioned “Bill Conlin's work” and contained

complaints about the sports writing of Bill Conlin and his failure to criticize the Philadelphia Phillies baseball team for the way that they handle their payroll.

43. As a result, K.R.'s e-mail in box received approximately 60,000 "bounced" e-mail messages and The Sporting News had to close his e-mail account and open a new one to deal with the problem.

Attack of September 2, 2002

44. On or about September 2, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer that was used by Cable One as a mail server and launched another attack. The e-mail was on the subject "The Scam Gets Busy" and again criticized the newspapers for failing to criticize the Philadelphia Phillies baseball team for the way that they handled their payroll issues. He spoofed the return e-mail address of D.D., a reporter at Fox Sports. As a result, Fox Sports had to change the e-mail address of D.D.

Attempted Attack of September 4, 2002

45. On or about September 4, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Armstrong Cable Services, an ISP in Butler, PA, without the permission of the owner, and launched another e-mail attack. The subject line of this e-mail was, "The Scam Gets Busy" and he again spoofed the return address of D.D. of Fox Sports. However, because Fox Sports had already changed the e-mail address of D.D., there was no flood of e-mails in any e-mail box at the Fox Sports server.

Attack of September 10, 2002

46. On or about September 10, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Cablevision, without the permission of the owner, and launched another e-mail attack. The subject line of this e-mail was, "The Big Lie." He spoofed the return e-mail address of J.B., a reporter at ESPN Sports.

47. On or about September 10, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Armstrong Cable Services without the permission of the owner, and launched another e-mail attack. The subject line of this e-mail was again, "The Big Lie." The text was the same as the e-mail referred to in the preceding paragraph. He again spoofed the return e-mail address of J.B.

Attack of September 16-19, 2002

48. Between on or about September 16, 2002, and on or about September 19, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Comcast, in Philadelphia, Pennsylvania, without the permission of the owner, and launched another e-mail attack. The subject line of this e-mail was "Wolf Goes Public." The content of this e-mail involved trades and acquisitions of players by the Philadelphia Phillies. The defendant spoofed the e-mail address of D.R., a sports writer at ESPN Magazine.

Attack of September 30, 2002

49. On or about September 30, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Comcast, without the permission of the owner, and launched another e-mail attack. The subject of the e-mail was, "The Scam Gets Busy Again." The e-mail criticized the sports writers at the Philadelphia newspapers for being apologists for the owners of the Philadelphia Phillies. The defendant spoofed the e-mail address of L.S., of the staff of PNI. As a result, more than 49,000 copies of this e-mail were "bounced" to the e-mail box of L.S.

Attack of October 8-9, 2002

50. On or about October 8 and 9, 2002 the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Comcast, without the permission of the owner, and launched another e-mail attack. The subject of the e-mail was, "Jim Buck, Jr. Makes a New Investment." CARLSON spoofed the e-mail return address of T.K., a reporter at ESPN magazine.

Attack of December 5, 2002

51. On or about December 5, 2002, the defendant ALLAN ERIC CARLSON gained unauthorized access over the Internet to a computer owned by a subscriber of Comcast, without the permission of the owner, and launched another e-mail attack. He spoofed an e-mail address at the Phillies. The e-mail message quoted from a Philadelphia Inquirer newspaper article regarding the arrest and subsequent discharge of a Philadelphia Phillies player on domestic violence charges. As a result, the computer network of the Philadelphia Phillies received more than 27,000 "bounced" copies of this e-mail.

THE CHARGES

52. On or about each of the dates listed below (each date constituting a separate count of this indictment), at Philadelphia in the Eastern District of Pennsylvania, and elsewhere, the defendant

ALLAN ERIC CARLSON

knowingly caused the transmission of information and code, that is e-mail messages, and as a result of such conduct intentionally caused and attempted to cause damage without authorization to protected computers, that is the defendant launched an e-mail attack that affected the integrity and availability of data on the protected computers listed below, and by this conduct, together with other acts committed in a related course of conduct, described in Paragraphs 7 through 18 of Counts One through Eleven, caused a loss to PNI and the Philadelphia Phillies aggregating more than \$5,000, during the time period from on or about November 7, 2001 up to and including on or about December 31, 2001.

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	OWNER OF THE PROTECTED COMPUTER
1	11/07/2001	7	PNI
2	11/11/2001	8	Phillies
3	11/13/2001	9	Phillies
4	11/16/2001	10	PNI, Phillies
5	11/18/2001	11, 12	PNI, Phillies
6	11/19/2001	13	Phillies
7	11/19/2001	13	PNI

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	OWNER OF THE PROTECTED COMPUTER
8	11/20/2001	14	PNI
9	12/03/2001	15	PNI
10	12/09/2001	16	PNI
11	12/10/2001	17, 18	PNI

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i) and 1030(b).

COUNTS 12 THROUGH 26

THE GRAND JURY FURTHER CHARGES:

1. Paragraphs 1 through 51 of Counts One through Eleven are incorporated by reference.

2. On or about each of the dates listed below (each date constituting a separate count of this indictment), at Philadelphia in the Eastern District of Pennsylvania, and elsewhere, the defendant

ALLAN ERIC CARLSON

knowingly caused the transmission of information and code, that is e-mail messages, and as a result of such conduct intentionally caused and attempted to cause damage without authorization to protected computers, that is, the defendant launched an e-mail attack which affected the integrity and availability of data on the protected computers listed below, and by this conduct, together with other acts committed in a related course of conduct, described in Paragraphs 19 through 51 of Counts One through Eleven, caused a loss to PNI and the Philadelphia Phillies aggregating more than \$5,000, during the time period from on or about January 1, 2002, up to and including on or about December 5, 2002.

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	OWNER OF THE PROTECTED COMPUTER
12	01/20/2002	19	PNI
13	01/24/2002	20	PNI
14	02/19/2002	21, 22	PNI

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	OWNER OF THE PROTECTED COMPUTER
15	02/26/2002	23	Phillies
16	03/12/2002	24, 25	Phillies
17	03/13/2002	26	PNI
18	06/17/2002	28	PNI
19	06/19/2002	29	PNI
20	07/01/2002	30, 31	PNI
21	07/14/2002	32	PNI
22	07/17/2002	33	PNI
23	07/20/2002	34, 35	PNI
24	08/01/2002	36	Phillies
25	09/30/2002	49	PNI
26	12/05/2002	51	Phillies

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i) and 1030(b).

COUNT 27 THROUGH 37

THE GRAND JURY FURTHER CHARGES:

1. Paragraphs 1 through 51 of Counts One through Eleven are incorporated by reference.

2. On or about each of the dates listed below (each date constituting a separate count of this Indictment), at Philadelphia in the Eastern District of Pennsylvania and elsewhere, the defendant

ALLAN ERIC CARLSON

intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused, and attempted to cause, damage, that is, he launched an e-mail attack, which affected the integrity and availability of data on the computers owned by the entities listed below and by this conduct, together with other acts committed in a related course of conduct, described in Paragraphs 7 through 18 of Counts One through Eleven, caused losses to PNI and the Philadelphia Phillies, aggregating more than \$5,000, during the time period from on or about November 7, 2001, up to and including on or about December 31, 2001.

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	PERSON SUFFERING DAMAGE
27	11/07/2001	7	PNI
28	11/11/2001	8	Phillies
29	11/13/2001	9	Phillies
30	11/16/2001	10	PNI, Phillies
31	11/18/2001	11, 12	PNI, Phillies

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	PERSON SUFFERING DAMAGE
32	11/19/2001	13	Phillies
33	11/19/2001	13	PNI
34	11/20/2001	14	PNI
35	12/09/2001	16	PNI
36	12/10/2001	17, 18	PNI
37	12/03/2001	15	PNI

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(ii), 1030(a)(5)(B)(i) and 1030(b).

COUNTS 38 THROUGH 52

THE GRAND JURY FURTHER CHARGES:

1. Paragraphs 1 through 51 of Counts One through Eleven are incorporated by reference.

2. On or about each of the dates listed below (each date constituting a separate count of this Indictment), at Philadelphia in the Eastern District of Pennsylvania and elsewhere, the defendant

ALLAN ERIC CARLSON

intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused, and attempted to cause, damage, that is, he launched an e-mail attack, which affected the integrity and availability of data on the computers owned by the entities listed below and by this conduct, together with other acts committed in a related course of conduct, described in Paragraphs 19 through 51 of Counts One through Eleven, caused losses to PNI and the Philadelphia Phillies, aggregating more than \$5,000, during the time period from on or about January 1, 2002, up to and including on or about December 5, 2002.

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	PERSON SUFFERING DAMAGE
38	01/20/2002	19	PNI
39	01/24/2002	20	PNI
40	02/19/2002	21, 22	PNI
41	02/26/2002	23	Phillies
42	03/12/2002	24, 25	Phillies

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	PERSON SUFFERING DAMAGE
43	03/13/2002	26	PNI
44	06/17/2002	28	PNI
45	06/19/2002	29	PNI
46	07/01/2002	30, 31	PNI
47	07/14/2002	32	PNI
48	07/17/2002	33	PNI
49	07/20/2002	34, 35	PNI
50	08/01/2002	36	Phillies
51	09/30/2002	49	PNI
52	12/05/2002	51	Phillies

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(ii), 1030(a)(5)(B)(i) and 1030(b).

COUNTS 53 THROUGH 79

THE GRAND JURY FURTHER CHARGES:

1. Paragraphs 1 through 51 of Counts One through Eleven are incorporated by reference.
2. From on or about each of the dates listed below (each date constituting a separate count of this Indictment), at Philadelphia in the Eastern District of Pennsylvania and elsewhere, the defendant

ALLAN ERIC CARLSON

knowingly used, without lawful authority, in and affecting interstate commerce, a means of identification of another person, that is the e-mail addresses of the persons listed below with the intent to commit and to aid and abet the commission of violations of Federal law, that is computer fraud, in violation of Title 18, United States Code, Section 1030 as charged in this indictment.

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	NAME OF PERSON WHOSE E-MAIL ADDRESS WAS USED
53	11/19/2001	13	P.H.
54	12/03/2001	15	P.H.
55	12/09/2001	16	B.B.
56	12/10/2001	17, 18	P.H.
57	01/20/2002	19	B.B.
58	01/24/2002	20	B.B.
59	02/19/2002	21, 22	T.D.
60	02/19/2002	21, 22	B.M.
61	02/19/2002	21, 22	P.M.
62	02/19/2002	21, 22	J.M.

COUNT	DATE	RELATED PARAGRAPHS FROM COUNTS ONE THROUGH ELEVEN	NAME OF PERSON WHOSE E-MAIL ADDRESS WAS USED
63	02/19/2002	21, 22	A.M.
64	02/19/2002	21, 22	L.S.
65	02/19/2002	21, 22	A.R.
66	02/19/2002	21, 22	C.S.
67	02/19/2002	21, 22	G.S.
68	02/19/2002	21, 22	T.S.
69	02/19/2002	21, 22	J.T.
70	02/19/2002	21, 22	R.T.
71	02/19/2002	21, 22	F.V.
72	02/19/2002	21, 22	R.W.
73	03/13/2002	26	L.S.
74	06/17/2002	28	P.H.
75	07/01/2002	30, 31	C.S.
76	07/14/2002	32	P.M.
77	07/17/2002	33	P.M.
78	07/20/2002	34, 35	R.W.
79	09/30/2002	49	L.S.

All in violation of Title 18, United States Code, Section 1028(a)(7).

NOTICE OF FORFEITURE

As a result of the violation of Title 18, United States Code, Section 1028 set forth in Counts 53 through 79 of this Indictment, the defendant

ALLAN ERIC CARLSON

shall forfeit to the United States under Title 18, United States Code, Section 1028(b)(5) any property used and intended to be used to commit these offenses, including but not limited to the following:

One NEC desktop computer (serial number 7YA02418US)
five floppy disks
two CD-R disks

If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third person;
- (c) has been placed beyond the jurisdiction of the Court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 1028(g) and Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant listed above as being subject to forfeiture.

A TRUE BILL

FOREPERSON

PATRICK L. MEEHAN
United States Attorney